



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/592,337	06/13/2000	Michael Marcovici	2-27	5543

46290 7590 11/19/2004

WILLIAMS, MORGAN & AMERSON/LUCENT
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 11/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	Application No. 09/592,337	Applicant(s) MARCOVICI ET AL.	
	Examiner Jung W Kim	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 7-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 7-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 March 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____. | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
6) <input type="checkbox"/> Other: _____. |
|---|--|

DETAILED ACTION

1. Claims 7-24 have been examined.

Response to Arguments

2. Applicant's arguments filed September 14, 2004 have been fully considered but they are not persuasive. In regards to Applicants claim the prior art of record does not teach authenticating the mobile shell having an established security association with the server network based upon the first message and a first key known to the user identity module and unknown to the mobile shell, and further that prior art of record teaches away from these limitations (see amendment, page 4, first full paragraph), examiner disagrees. Admission teaches establishing a security association between a mobile shell communicatively coupled with a user identity module and network (see admission, page 5, line 20-page 6, line 18). Admission clearly discloses the security association interaction occurring between the user identity module (USIM) and the network (specifically the VLR) using, inter alia, the secret key k_i known only to the subscriber's USIM and the VLR: the mobile shell does not have access to this secret key k_i since only the USIM identifies a specific subscriber. See admission, page 3, lines 9-11; page 5, lines 1-9, especially lines 1-3. Further, when the handshake between the USIM and VLR concludes successfully, a security association is then established between the mobile shell and network. See admission, page 6, lines 20-21.

Art Unit: 2132

3. Further, Mizikovsky teaches a challenge/response scheme to periodically authenticate the mobile station to the server network for increased security. See Mizikovsky, col. 3, line 61-col. 4, line 2; col. 6, lines 47-65; especially lines 50-51. Since, as stated earlier, admission teaches the initial security association between the mobile station and server network is processed by the USIM and the VLR (only the USIM identifies a unique subscriber, and the USIM stores and processes all security algorithms and key values to authenticate the mobile shell; see admission, page 2, lines 20-23 and page 3, lines 5-11), any successive authentication steps between the mobile shell and server network would also occur between the USIM and VLR, using key values only known to the USIM and VLR. For these reasons and those stated below, the prior art of record cover the limitations of the claimed invention.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

Art Unit: 2132

not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 7-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art in the applicants specification: "Description of Related Art" (hereinafter admission) in view of Mizikovsky et al. U.S. Patent No. 5,794,139 (hereinafter Mizikovsky).

7. As per claim 16, admission discloses a method of establishing a security association between a server network and a mobile shell communicatively coupled with a user identity module (see admission, page 3, line 1-page 7, line 16), the method comprising:

- a. establishing a security association with the mobile shell (see admission, page 5, line 20-page 6, line 18).

Admission specifically details an established AKA challenge/response scheme using a random number (RAND) generated by the network server and a secret key known by the server network and the user identity module but unknown to the mobile shell to create a response by the user identity module (RES) and an expected response by the server network (XRES) to establish this security association. However, admission does not disclose authenticating the mobile shell once a security association exists between the mobile shell and the server network. Mizikovsky teaches a system wherein a

Art Unit: 2132

challenge/response scheme is implemented to periodically authenticate the mobile station to the server network (see Mizikovsky, col. 3, line 61-col. 4, line 2; col. 6, lines 47-65). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Mizikovsky to the method of admission. Motivation for combination enables a more secure system by periodically authenticating the mobile shell. Hence, the invention of admission as modified by Mizikovsky further comprises:

- b. receiving a first message from the mobile shell (see Mizikovsky, col. 3, lines 66-67);
- c. authenticating the mobile shell based upon the first message and a first key known to the user identity module and unknown to the mobile shell (see admission, page 5, lines 10-26; page 6, lines 12-18 as modified by Mizikovsky, col. 4, lines 1-2; col. 6, lines 47-65).

The aforementioned covers claim 16.

8. As per claim 17, admission as modified by Mizikovsky covers a method as outlined above in the claim 16 rejection under 35 U.S.C. 103(a). In addition, the step of receiving the first message from the mobile shell further comprises:

- a. providing a second message to the mobile shell after the security association has been established (see Mizikovsky, col. 3, lines 61-66); and
- b. receiving the first message in response to the second message (see Mizikovsky, col. 3, line 66-col. 4, line 2).

The aforementioned cover the limitations of claim 17.

9. As per claim 18, admission as modified by Mizikovsky covers a method as outlined above in the claim 17 rejection under 35 U.S.C. 103(a). In addition, the step of providing the second message further comprises providing at least one of a unique challenge interrogation message and a global challenge interrogation message. See Mizikovsky, col. 6, lines 47-65. The aforementioned cover the limitations of claim 18.

10. As per claim 19, admission as modified by Mizikovsky covers a method as outlined above in the claim 17 rejection under 35 U.S.C. 103(a). In addition, the step of providing the second message further comprises providing a random number. See Mizikovsky, col. 3, lines 60-66. The aforementioned cover the limitations of claim 19.

11. As per claim 20, admission as modified by Mizikovsky covers a method as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the step of receiving the first message further comprises receiving a first message formed by the user identity module based upon the random number and the first key known to the user identity module and not known to the mobile shell. See admission, page 5, lines 10-26; page 6, lines 1-18; see Mizikovsky, col. 4, lines 1-2. The aforementioned cover the limitations of claim 20.

12. As per claim 21, admission as modified by Mizikovsky covers a method as outlined above in the claim 17 rejection under 35 U.S.C. 103(a). In addition, the server

Art Unit: 2132

network generates an expected response, compares it to the received response, and authenticates the mobile shell if the expected response is equal to the received response. See Mizikovsky, col. 3, line 66-col. 4, line 2; col. 6, lines 47-65. The aforementioned cover the limitations of claim 21.

13. As per claim 22, admission as modified by Mizikovsky covers a method as outlined above in the claim 21 rejection under 35 U.S.C. 103(a). In addition, the step of determining the fifth message comprises applying a non-reversible algorithmic function to the portion of the second message and the first key known to the user identity module and not known to the mobile shell. See admission, page 4, lines 22-31; see Mizikovsky, col. 3, lines 61-66. The aforementioned cover the limitations of claim 22.

14. As per claim 23, admission as modified by Mizikovsky covers a method as outlined above in the claim 16 rejection under 35 U.S.C. 103(a). In addition, the step of receiving the first message comprises receiving a third message formed by the user identity module based upon the first key and a fourth message formed by the mobile shell using a second key known to the mobile shell. See admission, page 6, line 20-page 7, line 16 wherein the second key is 'IK'. The aforementioned cover the limitations of claim 23.

15. As per claim 24, admission as modified by Mizikovsky covers a method as outlined above in the claim 23 rejection under 35 U.S.C. 103(a). In addition, the step of

Art Unit: 2132

authenticating the mobile shell based upon the first message and the first key known to the user identity module and not known to the mobile shell further comprises:

- a. generating a sixth message based upon the first and second keys (see admission, page 5, line 28-page 6, line 17; page 6, line 20-page 7, line 16 wherein second key is 'IK'; see Mizikovsky, col. 6, lines 46-65);
- b. comparing the first message and the sixth message and authenticating the mobile shell when a portion of the first message is equal to a portion of the sixth message (see Mizikovsky, col. 4, lines 1-2).

The aforementioned cover the limitations of claim 24.

16. As per claims 7-12 and 14, they are method claims corresponding to the inventions covered in the claim 16-24 rejections and they do not teach or define above the information covered in the claim 16-24 rejections. Therefore, claims 7-12 and 14 are rejected as being unpatentable over admission in view of Mizikovsky for the same reasons set forth in the rejections of claims 16-24.

17. As per claim 13, admission as modified by Mizikovsky covers a method as outlined above in the claim 12 rejection under 35 U.S.C. 103(a). In addition, the second key is an integrity key. The aforementioned cover the limitations of claim 13.

18. As per claim 15, admission as modified by Mizikovsky covers a method as outlined above in the claim 7 rejection under 35 U.S.C. 103(a). In addition, the step of

Art Unit: 2132

determining the second message based upon the first key known to the server network and not known to the mobile shell comprises determining the second message based upon an anonymity key known to the server network and not known to the mobile shell. See admission, page 5, lines 10-18, wherein 'AK' is anonymity key. The aforementioned cover the limitations of claim 15.

Conclusion

19. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Telephonic Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Jung W Kim
Examiner
Art Unit 2132

Jk
November 9, 2004



GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100